

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

UNITED STATES OF AMERICA)
)
 v.)) Criminal No. 21-110
)
 KHALED MIAH,)
)
 Defendant.)

MEMORANDUM OPINION

I. **BACKGROUND**

Defendant Khaled Miah is charged in an eight-count Indictment with the following: five counts of making interstate threats to injure FBI agents, in violation of 18 U.S.C. § 875(c); two counts of influencing and/or retaliating against FBI agents by threat, in violation of 18 U.S.C. § 115(a)(1)(B); and one count of altering and deleting records in a federal investigation, in violation of 18 U.S.C. § 1519. (Docket No. 33). Jury selection and trial are scheduled to commence on December 7, 2021. (Docket No. 109). Presently before the Court are four Motions in Limine regarding the admissibility at trial of business records of Twitter, Inc., Apple Inc., Facebook, Inc., and an Electronic Tracking Device, each of which is opposed by Defendant. (Docket Nos. 153; 155; 156; 158; 176-179; 195). For reasons that follow, each of the Government's Motions will be denied.

II. TWITTER, FACEBOOK AND APPLE RECORDS

The Government moves to admit at trial business records of Twitter, Facebook, and Apple pursuant to Federal Rules of Evidence 902(11)¹ and 803(6).² (*See* Docket Nos. 153, 155, 156). The Government submits that the records meet the requirements for self-authentication under Rule 902(11) and admissibility under Rule 803(6), thus they should be admitted without the need for the Government to call a records custodian to testify at trial. (Docket Nos. 153 at 2; 155 at 2; 156 at 2). In support, the Government submits the following: the records were produced in discovery to Defendant; Twitter provided a business records certification of authenticity dated October 1, 2021, Facebook provided a certification of authenticity dated January 10, 2021, and Apple provided a certification of authenticity dated May 28, 2020;³ and, the Government provided Defendant with notice of its intention to introduce the records through the certifications and the written Motions in Limine. (Docket Nos. 153 at 1, 2; 153-2; 155 at 1, 2; 155-2; 156 at 1, 2; 156-2). Additionally, the Government intends to supplement the certifications with evidence at trial

¹ Rule 902(11) provides that “[t]he original or a copy of a domestic record that meets the requirements of Rule 803(6)(A)-(C), as shown by a certification of the custodian or another qualified person that complies with a federal statute or a rule prescribed by the Supreme Court” is “self-authenticating” and “require[s] no extrinsic evidence of authenticity in order to be admitted.” Fed. R. Evid. 902(11). The rule requires that, “[b]efore the trial or hearing, the proponent must give an adverse party reasonable written notice of the intent to offer the record--and must make the record and certification available for inspection--so that the party has a fair opportunity to challenge them.” (*Id.*).

² Rule 803(6) specifies that records of a regularly conducted activity are an exception to the rule against hearsay, regardless of whether the declarant is available as a witness. Fed. R. Evid. 803(6). A record of a regularly conducted activity is a record of an act, event, condition, opinion, or diagnosis if: (A) the record was made at or near the time by--or from information transmitted by--someone with knowledge; (B) the record was kept in the course of a regularly conducted activity of a business, organization, occupation, or calling, whether or not for profit; (C) making the record was a regular practice of that activity; (D) all these conditions are shown by the testimony of the custodian or another qualified witness, or by a certification that complies with Rule 902(11) or (12) or with a statute permitting certification; and (E) the opponent does not show that the source of information or the method or circumstances of preparation indicate a lack of trustworthiness. (*Id.*).

³ The Government states in its Motion that Apple provided a business records certification of authenticity dated May 28, 2021. (Docket No. 155 at 1). The certification attached to the Government’s Motion is dated May 28, 2020. (Docket No. 155-2).

attributing the Twitter, Facebook and Apple iCloud accounts to Defendant. (Docket Nos. 153 at 2; 155 at 2; 156 at 2).

Defendant responds that “[t]he business records affidavit the government puts forth does not authenticate the Twitter [and Facebook] communications or posts themselves; the records custodians can only attest to the accuracy of the platform at the time of the production.” (Docket Nos. 176 at 3; 178 at 3). Accordingly, Defendant maintains that his Twitter and Facebook posts and records are not admissible as business records under Rules 803(6) and 902(11) pursuant to *United States v. Browne*, 834 F.3d 403 (3d Cir. 2016). (Docket Nos. 176 at 3; 178 at 3).

As to the Apple records, “the defense will stipulate as to the *authenticity* of [those] records (returns), agreeing that the data returned by Apple is what was in [Defendant’s] account – i.e., that it belonged to him.” (Docket No. 177 at 1) (emphasis in original). However, the defense does not stipulate to the admissibility of the Apple returns. (*Id.*). According to Defendant, Rules 902 and 803(6) are intertwined - for evidence to be admissible under Rule 902(11), the evidence must also meet the requirements for admissibility under Rule 803, but the Apple returns do not in this case. (*Id.*). Defendant points out that Apple iCloud is a storage platform, thus it only stored the documents it supplied and did not create them. (*Id.* at 2-3). As such, “the Apple returns fail the test under Rule 803(6) and are therefore not business records.” (*Id.* at 3). Accordingly, Defendant advocates that the Apple records are not admissible as business records under *Browne*.

In accordance with *Browne*, wherein the Third Circuit Court of Appeals addressed the proper authentication of social media records, the Twitter, Facebook and Apple records are not business records that qualify for self-authentication under Rule 902(11).

As background, the defendant in *Browne* appealed his conviction of child pornography and other sexual offenses on the basis that Facebook “chat logs,” containing messages exchanged

between an email account that he had access to and various minor victims, were not properly authenticated pursuant to Rule 902(11). *Browne*, 834 F.3d at 405-06. Facebook provided the chat logs and a certificate of authenticity executed by its records custodian. *Id.* at 406. In accordance with Federal Rule of Evidence 902(11), the certificate stated that the records produced by Facebook for the named accounts met the business records requirements of Rule 803(6)(A)-(C). *Id.*

On appeal, the defendant argued that the Facebook records were not properly authenticated because the Government failed to establish that he was the person who authored the communications. *Browne*, 834 F.3d at 408. The Government argued that the Facebook records are business records that were properly authenticated pursuant to Rule 902(11) by a certificate from Facebook's records custodian. *Id.* As the Third Circuit Court of Appeals explained the issue, “[t]he viability of the Government’s position turn[ed] on whether Facebook chat logs are the kinds of documents that are properly understood” as business records under Rule 803(6), such that they qualify for self-authentication under Rule 902(11). *Id.* at 409. The Court of Appeals concluded that they are not. *Id.*

In so ruling, the *Browne* Court observed that the “Government’s theory of self-authentication . . . is predicated on a misunderstanding of the business records exception.” *Browne*, 834 F.3d at 410. “Rule 803(6) is designed to capture records that are likely accurate and reliable in content, as demonstrated by the trustworthiness of the underlying sources of information and the process by which and purposes for which that information is recorded.” *Id.* at 410. Applying this principle to the facts, the Court of Appeals elaborated as follows:

Facebook does not purport to verify or rely on the substantive contents of the communications in the course of its business. At most, the records custodian employed by the social media platform can attest to the accuracy of only certain aspects of the communications exchanged over that

platform, that is, confirmation that the depicted communications took place between certain Facebook accounts, on particular dates, or at particular times. This is no more sufficient to confirm the accuracy or reliability of the contents of the Facebook chats than a postal receipt would be to attest to the accuracy or reliability of the contents of the enclosed mailed letter.

Id. at 410-11. Consequently, the Court of Appeals held that, “considered in their entirety, the Facebook records are not business records under Rule 803(6) and thus cannot be authenticated by way of Rule 902(11).”⁴ *Id.* at 411.

Browne’s rationale and holding that Facebook records are not business records under Rule 803(6) applies equally to the Twitter, Facebook and Apple records at issue here. Thus, the Government cannot authenticate and admit the **content** of Defendant’s Facebook and Twitter accounts or stored in his Apple iCloud account relying solely on certifications from the records custodians of those companies. Accordingly, the Government’s Motions to admit those records pursuant to Federal Rules of Evidence 902(11) and 803(6) will be denied.

III. ELECTRONIC TRACKING DEVICE RECORDS

The Government also moves to admit at trial business records of the Federal Bureau of Investigation’s Geospatial Information Systems Program’s Electronic Tracking Device pursuant

⁴ Despite concluding that the Facebook chat logs were not properly authenticated under Rule 902(11), the *Browne* Court found that the record contained abundant evidence linking the defendant and the testifying victims to the chats conducted through the Facebook account and reflected in the logs obtained from Facebook, thus the Facebook records were duly authenticated under Rule 901(a). *Browne*, 834 F.3d at 413-15. In so ruling, the Court of Appeals held that “it is no less proper to consider a wide range of evidence for the authentication of social media records than it is for more traditional documentary evidence.” *Id.* at 412. After reviewing the extrinsic evidence presented by the Government, the Court of Appeals commented that the Government not only provided ample evidence linking the defendant to the Facebook account, but also supported the accuracy of the chat logs by obtaining them directly from Facebook and introducing a certificate attesting to their maintenance by Facebook’s automated systems. *Id.* at 414. “To the extent that certified records straight from the third-party service provider are less likely to be subject to manipulation or inadvertent distortion . . . the method by which the government procured the records . . . constitutes yet more circumstantial evidence that the records are what the Government claims.” *Id.* at 414-15. Consistent with *Browne*, it is entirely appropriate for the Government to rely on certifications in establishing authenticity under Rule 901(a).

to Federal Rules of Evidence 902(11), 902(13)⁵ and 803(6). (See Docket No. 158). The Government maintains that the records meet the requirements for self-authentication under Rules 902(11) and 902(13) and admissibility under Rule 803(6), thus they should be admitted without the need for the Government to call a records custodian to testify at trial. (*Id.* at 3). In support, the Government submits that the records were produced in discovery to Defendant, the FBI provided a business records certification of authenticity and declaration dated October 14, 2021, and the Government provided Defendant with notice of its intention to introduce the records through the certification and the written Motion in Limine. (*Id.* at 1, 2; Docket No. 158-2). Additionally, the Government intends to present evidence showing that the electronic tracking device was attached to Defendant's vehicle pursuant to a federal search warrant. (Docket No. 158 at 1).

Defendant responds that the Government's request to admit the electronic tracking device returns as business records should be denied because: tracking data is not a business record; and the data was created by the Government for litigation purposes, thus it is testimonial and admission without a sponsoring witness violates the Confrontation Clause. (Docket No. 179 at 1, 4). As background, Defendant says that the FBI attached the tracking device to his vehicle pursuant to a warrant executed on November 20, 2020, for a period of 45 days. (*Id.* at 1). During that time, the Government supposedly was preparing to indict Defendant for allegedly violating 18 U.S.C. § 2261A (stalking). (*Id.*). Subsequently, on December 30, 2020, a second warrant, which was executed after Defendant posted four of the five alleged threats and as the Government prepared

⁵ Rule 902(13), which pertains to certified records generated by an electronic process or system, provides that “[a] record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12)” is self-authenticating. Fed. R. Evid. 902(13). Pursuant to the rule, the proponent must also meet the notice requirements of Rule 902(11). *Id.*

to indict him on the pending charges, extended the period for an additional 45 days. (*Id.* at 1-2). Given this background, Defendant contends that data obtained from the tracking device was obtained in anticipation of litigation, *i.e.*, for the purpose of establishing or proving some fact at trial, and therefore is not admissible as a business record. (*Id.* at 2). According to Defendant, the tracking data is testimonial in nature and thus is subject to confrontation under the Sixth Amendment. (*Id.* at 2-3).

In reply, the Government counters that admission of the tracking data, which is “raw data,” does not violate the Confrontation Clause because the data is not testimonial. (Docket No. 195 at 1, 3). First, it is electronic data created by an automated process, which is not the functional equivalent of *ex parte* in court testimony. (*Id.* at 1). According to the Government, “[i]t is simply data produced by a computer” not a “solemn declaration or affirmation made for the purpose of establishing or proving some fact.” (*Id.*). Although the Government has provided an affidavit from the witness certifying the data, the affidavit only was provided to satisfy the requirements of Rule 902(13). (*Id.* at 2). Because that witness is only authenticating data, there is no need to subject him to cross-examination. (*Id.*). The Government emphasizes that “[t]he people who will draw conclusions from that data and explain what it shows are the FBI agents who interpreted it. They will testify at trial and be available for cross-examination.” (*Id.* at 3).

Even if electronically produced data could be considered testimonial, the Government further submits that it would not be here because the data was not made in anticipation of a trial. (Docket No. 195 at 2). The Government explains that the tracker was placed on Defendant’s vehicle after Defendant allegedly targeted an FBI Special Agent’s wife online, and “allowed the FBI to keep watch of an individual it considered dangerous to safeguard the agent’s wife and others,” not to obtain evidence for a trial. (*Id.*).

In analyzing this issue, the Court initially observes that Defendant cites no authority to support his contention that tracking data is not a business record. (See Docket No. 179 at 1). Contrary to Defendant's position, a number of courts have held that electronic tracking data is admissible as a business record under Rule 803(6). *See United States v. Veloz*, 948 F.3d 418, 433 (1st Cir. 2020) (GPS tracking data that was created and stored contemporaneously with the defendant's conduct was not in preparation for litigation, and therefore business records exception encompassed that data in trial on charge of conspiracy to commit kidnapping, although the government's trial exhibit that set forth GPS data was prepared in anticipation of litigation); *United States v. Brooks*, 715 F.3d 1069, 1079 (8th Cir. 2013) (GPS reports tracking bank robber fell under business records exception to admission of hearsay evidence, since security systems provider routinely kept GPS data on company server as part of regular course of business upon customer's activation of GPS device); *United States v. Wood*, No. 08-CR-92A, 2009 WL 2157128, at *4 (W.D.N.Y. July 15, 2009) (GPS records satisfied requirements of the business records exception). The Court finds persuasive this authority and similarly concludes that the tracking device data here meets the requirements of a business record under Rule 803(6). (See Docket No. 158-2).

Turning to authentication of the tracking device data, as discussed, Defendant maintains that the data is testimonial, thus admission without a sponsoring witness violates the Sixth Amendment's Confrontation Clause. (Docket No. 179 at 1). Based on information presently available to the Court, it is questionable whether the tracking device data is testimonial; however, out of caution, authentication by a records custodian will be required at trial for reasons explained below.

As a general matter, most business records under Rule 803(6) are non-testimonial statements to which the Confrontation Clause does not apply. To that end, in *Crawford v. United*

States, 541 U.S. 36 (2004), the Supreme Court held that only “testimonial” hearsay implicates the Confrontation Clause and observed that most of the traditional hearsay exceptions “covered statements that by their nature were not testimonial - for example, business records.” *Id.* at 56. Subsequently, the Supreme Court observed in *Melendez-Diaz v. Massachusetts*, 557 U.S. 305 (2009) that business and public records “are generally admissible absent confrontation . . . because - having been created for the administration of an entity’s affairs and not for the purpose of establishing or proving some fact at trial - they are not testimonial.” *Id.* at 324. As the Supreme Court explained in *Bullcoming v. New Mexico*, 564 U.S. 647 (2011), “[t]o rank as ‘testimonial,’ a statement must have a ‘primary purpose’ of ‘establish[ing] or prov[ing] past events potentially relevant to later criminal prosecution.’ ” *Id.* at 659, n.6 (quoting *Davis v. Washington*, 547 U.S. 813, 822 (2006)).

Nonetheless, certain business records still may run afoul of the Confrontation Clause if they are testimonial in nature. *See Bullcoming*, 564 U.S. at 669 (Sotomayor, J., concurring) (“To determine if a statement is testimonial, we must decide whether it has ‘a primary purpose of creating an out-of-court substitute for trial testimony.’ ” (quoting *Michigan v. Bryant*, 562 U.S. 344, 358 (2011)). According to Defendant, the FBI initially attached a tracking device to his vehicle pursuant to a federal search warrant on November 20, 2020, and collected tracker data during November and December of 2020, when the Government supposedly was preparing to indict him for stalking. (Docket No. 179 at 1). On December 30, 2020, a second warrant, which was executed after Defendant posted four of the five alleged threats and as the Government prepared to indict him on the pending charges, extended the period for an additional 45 days. (*Id.* at 1-2). As a result, Defendant argues that “[d]ata obtained from the Electronic Tracking Device . . . was clearly obtained in anticipation of litigation” and therefore is testimonial. (*Id.*).

Conversely, the Government contends that even if the tracker data could be considered testimonial, the data would not be here because it was not made in anticipation of a trial given that “the primary purpose of the tracker data was to keep track of a person the FBI considered dangerous and an immediate risk to an agent’s spouse.” (Docket No. 195 at 2-3).

In resolving the parties’ disagreement whether the tracking device data implicates the Confrontation Clause, “the crucial inquiry is whether the record was ‘created . . . for the purpose of establishing or proving some fact *at trial.*’” *Brooks*, 715 F.3d at 1079 (quoting *Melendez-Diaz*, 557 U.S. at 324 (emphasis added)). As the *Brooks* court observed, the Supreme Court “has specifically held that certain statements obtained in the course of a law enforcement investigation may nonetheless be non-testimonial.” *Id.* at 1079-80 (citing *Bryant*, 562 U.S. at 376 (holding that shooting victim’s statements to police regarding his shooting were non-testimonial statements because police “solicited the information necessary to enable them to meet an ongoing emergency”) (citation and internal quotation marks omitted); *Davis*, 547 U.S. at 826-27 (holding that victim’s statements to a 9-1-1 operator were non-testimonial as they “were necessary to be able to resolve the present emergency”) (emphasis omitted)). Consistent with this Supreme Court precedent, the *Brooks* court reasoned that the GPS tracking reports at issue were used to track the defendant in an ongoing pursuit, and, although they ultimately were used to link him to a bank robbery, they were not created for that purpose or to otherwise establish some fact at trial. *Id.* at 1080. Given that the GPS evidence was generated by the bank’s security company for the purpose of locating a robber and recovering stolen money, the *Brooks* court held that the GPS reports were non-testimonial, and their admission did not violate the defendant’s Confrontation Clause rights.⁶ *Id.*

⁶ The *Brooks* court additionally noted that the GPS tracking reports at issue were distinguishable from the chemical analysis reports in *Melendez-Diaz* and the blood alcohol analysis in *Bullcoming* “because the operation of

In view of this authority, to the extent that the “primary purpose of the tracker data was to keep track of a person the FBI considered dangerous and an immediate risk to the agent’s spouse,” and it was not made to establish or prove some fact at trial, as the Government submits, the tracker data would be non-testimonial and would not run afoul of the Confrontation Clause. The non-testimonial nature of the proffered tracker data appears to be corroborated by the fact that it is presumably generated by computer-based technology which would not involve specialized skill where human error could be possible. *See Brooks*, 715 F.3d at 1069. At this juncture, however, the information available to the Court consists only of the parties’ competing representations as to the purpose of the tracker data, without evidentiary support. Consequently, although it likely may be that the tracker data in question is raw data which is not testimonial, the Court is compelled to conclude, based on the present record, that authentication by a records custodian will be required at trial.⁷

the lab machines used in those cases required specialized skill with human error possible at each step.” *Brooks*, 715 F.3d at 1080, n.4 (citing *Bullcoming*, 564 U.S. at 653, 660; *Melendez-Diaz*, 557 U.S. at 318-21). In contrast, the GPS tracking reports in *Brooks* “were merely computer printouts of information generated by accepted technology. There was no human analysis. . . .” *Id.*

⁷ Despite this conclusion, the Court feels compelled to note one additional point concerning the necessity of a records custodian testifying at trial to authenticate business records of the electronic tracking device (or other business records). The Court is aware that the parties attempted to resolve issues surrounding the authenticity of the various business records through stipulations, presumably to avoid unnecessary time and expense on those matters at trial. Ultimately, that did not occur, given the motion practice that followed. Of course, the parties certainly are not required to stipulate on these, or any other, matters. Nonetheless, the Court reminds the parties that the Federal Rules of Criminal Procedure “are to be interpreted to provide for the just determination of every criminal proceeding, to secure simplicity in procedure and fairness in administration, and to eliminate unjustifiable expense and delay.” Fed. R. Crim. P. 2. Given this dictate, to the extent the parties wish to reconsider the prudence of using valuable trial time for a custodian to provide foundation testimony for the authenticity of the records, they are certainly encouraged to confer and advise the Court at the pretrial conference whether proceeding in that manner remains necessary.

IV. CONCLUSION

For the reasons stated herein, the Government's Motions in Limine regarding the business records of Twitter, Apple, Facebook and an Electronic Tracking Device (Docket Nos. 153, 155, 156, 158) each are denied.

An appropriate Order follows.

s/ W. Scott Hardy

W. Scott Hardy

United States District Judge

Date: November 22, 2021

cc/ecf: All counsel of record